AN ITC SECURE WHITE PAPER

THIRD-PARTY CYBER RISK: THE WEAKEST LINK

65% of cyber breaches originate from third parties

Organisations increasingly depend on vendors, partners, consultants and the like, to produce materials, to provide logistical support, to sell goods, to generate ideas, and more.

It could be said that these third-party suppliers 'oil the wheels of industry', and to make things run smoothly we make it as easy as possible for them to interact with us.

This interdependent relationship has spawned a new level of integration and trust. We give them privileged access to our data, we interface within bespoke supplier portals and share network connections. In doing this, we vastly increase the risks to our cyber security.

It is no coincidence that in the US, William Evanina, the Director of the National Counterintelligence and Security Center recently announced that "supply chain infiltration is one of the key threats that corporations need to pay attention to" and in the UK, Ciaran Martin, CEO at the National Cyber Security Centre named supply chain risk as one of his top 5 priorities that companies need to address when considering the protection of their own and customer data.

Highlighting the risks inherent in third-party relationships, this paper draws upon credible recent research to bring attention to the cyber threats all businesses face by simply doing business.

Cyber risk and the extended supply chain

Visibility of the extended supplier base is key to minimising the risk of a cyber-attack perpetrated from within a complex supply chain. But seeing into the supply chain to check for security preparedness can be a challenge. In a 2017 Ponemon study, 57% of respondents felt poor visibility into the supply chain left them unable to determine the effectiveness of vendors' security policies and measures.

This is all the more concerning when we consider that cyber security incidents doubled in 2017, and attacks such as the Debenhams and Equifax data breaches saw their origin in supply chain members and open source software.

We need to have visibility and quantitative metrics across our vendor supply chain to tease out the complexities of its structure. This will allow us to manage risk and extend our own security diligence to our third-party partners.

ITC Secure, Boatman's House, 2 Selsdon Way, London E14 9GL United Kingdom.
ITC Secure, 1701 Pennsylvania Avenue, NW Washington, DC 20006

Global enterprise is built on the back of a complex web of interconnected businesses. This extended community provides the backbone of innovation upon which modern business thrives. It is also the glue that holds commerce together, each part being intrinsically linked through technology and connectivity.

These technological changes, whilst being positive, are also changing the risk profile of all parties in the supply chain, adding new complexity to the threat landscape as never before. The more you connect the dots, the more vulnerabilities are exposed.

In fact, a recent report by The Ponemon Institute found that 65% of breaches originated at a third party with 75% of respondents saying that this figure is increasing.[2]

How third parties accumulate cyber security risks

Our web of partners, including suppliers, affiliates, contractors and service providers is a finely balanced environment that must be managed in order to optimise output. This extends to risk management which itself has many facets. Each link in the chain, in other words, each company in the system, has its own set of variables that need governance. But layered across this, are a number of cyber security threats and concerns that enter the chain. Here we take a look at some of the main contenders for the weakest link.

Phishing – Phishing, especially the highly targeted version, spear phishing, has been one of the most successful, and consequently, most used, types of cyber attack within a supply chain. You could call it the 'go to' tool of the cyber criminal. Often smaller suppliers (SMEs) will be targeted as a stepping-stone into the enterprise client. If an SME in the chain has privileged access to internal resources, the result is a compromised system.

Infected software – In the manufacturing sector there have been a series of attacks based on malware-infected industrial control systems (ICS). These attacks often begin with a phishing email into a supply chain member and end in an infected critical system. The attacks are multi-staged and often use remote Trojans to infect the very patches used to update security.[3]

Cloud and IoT – By 2020, Gartner expects that 90% of spending on supply chain management will be on Cloud solutions.[4] Coupled with internet-connected devices, this creates a very fluid and malleable cyber security matrix for the cybercriminal.

Watering hole attacks – These are based on compromising favoured sites within the extended supply chain. When anyone within the chain goes to the site, techniques, that are difficult to spot and control, such as 'Drive-by-Downloads' are used to infect the user's machine. Insidious malware known as a Remote Access Trojan (RAT) infection is often the outcome of such attacks. It works by stealth, infecting extended systems.

Mergers and acquisitions – The coming together of two or more organisations can often result in a clash of vendor supply chains. This can complicate an already complex cyber security matrix. Many exposure points can be overlooked during a merger, and imminent or on-going breaches lost in the M&A process.

Measure for measure

Traditional methods of measuring third-party risks rely heavily on "point in time" snapshots and heavy manual processes. Organisations generally identify third-party risk by periodically surveying their partners directly. Whilst this is a good start, it only provides a static snapshot of the organisation, and sifting through surveys is a long, manual process. It's no wonder that 83% of IT managers say they lack confidence in their existing third-party risk management programme.

ITC Secure, Boatman's House, 2 Selsdon Way, London E14 9GL United Kingdom.
ITC Secure, 1701 Pennsylvania Avenue, NW Washington, DC 20006

Measuring and managing risk across the chain

A more effective approach to addressing third-party risk that provides better information to organisations without an accompanying high cost should include:

Prioritising vendors and evaluating risk – First, organisations may have dozens or even hundreds of partners and will need to prioritise them based on risk. Start with a list of vendors and create a prioritised list based on an initial evaluation of their security posture, their importance to you, location, etc.

Understand infrastructure access and asset exchange – Pay particular attention to organisations which have access to your infrastructure, or with which you share confidential information or assets. Review not only the technology but also understand their policies and how well they follow and enforce them.

Integrate security and vendor procurement policies – Next, create your own governance around how you will review your third-parties, proper risk thresholds, and how you will address unmitigated risks. For example, define what is an acceptable risk and what isn't, and what you will do if a company will not fix a security issue. Publish these policies and review ways to reinforce them contractually.

Make it an ongoing process – It's important that you don't simply take a snapshot of an organisation's security situation and instead create an ongoing process to monitor your third-party relationships and their security posture on a regular, even monthly basis.

The importance of compliance

We all know that security attacks compromise data, expose intellectual property, and can cause irreparable brand, reputational and financial damage. But, beyond the remit of our own business, are we aware of our wider responsibility for those within our extended supply chain?

Cyber security is part of a gamut of regulations that businesses of all sizes need to comply with. This compliance extends to the management of cyber risk within the supply chain.

Many industry-specific and wider regulatory frameworks also require that supply chain members are checked and adhere to their requirements. Vendor risk management has to embrace compliance management. A few examples to demonstrate this are:

FCA[5] **Guidance for firms outsourcing to the 'cloud' and other third-party IT services** – It is the financial organisations responsibility to carry out a risk assessment to identify relevant risks, identify current industry good practice and document this process.

NIS Directive[6] – This covers the security of networks and information systems across essential services and infrastructures in the UK. The directive sets out:

"*It is the OES (Operator of Essential Services) responsibility to put in place appropriate and proportionate measures, and to ensure that their suppliers have in place appropriate measures, to manage risks of their services being disrupted via their supply chain.*"

HIPAA – In the U.S., security and privacy in the healthcare sector is managed through the Health Insurance Portability and Accountability Act (HIPAA). This was extended in 2013 to include the Omnibus Rule8 which requires that "business associates" are directly liable for compliance with some of the HIPAA privacy and security rules.

GDPR – The General Data Protection Regulation (GDPR) is EU-focused but impacts companies on a global scale. It is mirrored in the UK by the Data Protection Act 2018 (DPA). If your organisation is impacted by the GDPR or DPA, then personal data, no matter where in the life cycle or supply chain it is, has to comply with the requirements. If not, the fines are massive – up to 4% of global revenue or 20 million euros, whichever the greater.

ITC Secure, Boatman's House, 2 Selsdon Way, London E14 9GL United Kingdom.
ITC Secure, 1701 Pennsylvania Avenue, NW Washington, DC 20006

In conclusion

The threat landscape is ever evolving. While threats from legacy attacks still exist, the organisations need to evolve to protect against the current major threat to our cyber security – third-party risk.

Third-party cyber security risk across the extended supply chain is a real and serious issue. A report by insurance giant Allianz found that cyber risk and business interruption via the third parties was the risk that businesses were least prepared for.[7]

Organisations need to extend their thinking to close off the gaps in cyber security in the chain of third-party partners and affiliates. Managing the risk by monitoring how the extended supply chain acts and reacts to threats and vulnerabilities, is key to security vigilance. Monitoring and assessing third parties is crucial in this management exercise.

ITC offers a Gartner recommended third-party risk management and response service that brings visibility across the whole supply chain, together with the intelligence needed to track and quantify the risks of partners and suppliers. ITC acts as your eyes and ears, offering an outsider view of your third-party suppliers. We review systems, processes and infrastructure to offer an objective security score on a monthly basis. By monitoring alerts, we are able to offer real time support in responding to threats. As part of this service, our risk monitoring solution provides real-time alerts and detailed information on potential risks. With this level of knowledge, you can work with your third-party suppliers and partners to address and remediate issues, quickly and accurately – getting to the core of the problem before the cybercriminal hits.

References

(1) Online Trust Alliance: https://otalliance.org/news-events/press-releases/online-trust-alliance-reports-doubling-cyber-incidents-2017-0

(2) The Ponemon Institute, Data Risk in the Third-Party Ecosystem, 2017: https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/sep2017/cs2017_0340.pdf

(3) Hitachi, Dragonfly 2-0 Target Energy Sector Gaining Access to Scada Systems: https://www.hitachi-systems-security.com/blog/dragonfly-2-0-targets-energy-sector-gaining-access-to-scada-systems/

(4) Gartner blog: https://www.gartner.com/en/newsroom/press-releases/2017-06-22-gartner-says-supply-chain-management-market-will-exceed-13-billion-in-2017-up-11-percent-from-2016

(5) FCA Outsource Guidance: https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf

(6) NIS Directive Guidance: https://www.ncsc.gov.uk/guidance/nis-guidance-collection

(7) Allianz, A Guide to Cyber Risk: https://www.allianz.com/v_1441749600000/media/press/document/other/Allianz_Global_Corporate_Specialty_Cyber_Guide_final.pdf

ITC Secure, Boatman's House, 2 Selsdon Way, London E14 9GL United Kingdom.
ITC Secure, 1701 Pennsylvania Avenue, NW Washington, DC 20006